4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,485	09/29/2003	Fangguo Zhang	ZHAN3003 / EM	8456

23364 7590 02/06/2007

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
TO, BAOTRAN N	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/671,485	ZHANG ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending in the application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. (U.S. Patent 7,113,594 B2) hereinafter Boneh in view of Rivest, Shamir and Tauman (How to leak a secret, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.552-565, Springer-Verlag, 2001) hereinafter Rivest.

Regarding Claims 1 and 11, Boneh discloses a method for generating an identity-based ring signature by using bilinear pairings, in a cryptosystem that includes a user (receiver), a signer (sender) and a trusted authority (PKG 1003), which comprises the steps of:

at the trusted authority generating a set of system parameters (Parameters) shared by the user and the signer and storing the set of system parameters in a memory of each of the user and the signer (Abstract; Figure 10, col. 30, lines 17-28);

at the trusted authority, generating a public key and a private key for the user and the signer by using the set of system parameters, thereby transmitting the generated public and the private keys to the user and the signer through a secure channel, respectively (Figure 2, elements 220, 230, and 240, col. 15, lines 45-54);

at the user, concealing content of a message (col. 26, lines 28-40).

Boneh explicitly does not disclose "requesting a ring signature for the content-concealed message to the signer; at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message; and at the user, verifying validity of the ID-based ring signature."

However, RSA discloses requesting a ring signature for the content-concealed message to the signer (Abstract, page 552); at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message (pages 559-560); and at the user, verifying validity of the ID-based ring signature (pages 560-561).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Rivest's reference within Boneh to include requesting a ring signature for the content-concealed message to the signer; at the signer, producing the ring signature based on identity (ID) of the user, thereby forming an ID-based ring signature for the content-concealed message; and at the user, verifying validity of the ID-based ring signature. One of ordinary skill in the art would have been motivated to specify a set of possible signers without revealing which member actually produced the signature (Rivest, Abtract).

Regarding Claim 2, Boneh and Rivest disclose the limitations of Claim 1 above. Boneh further discloses wherein the step (a) includes the steps of: (a1) introducing a cyclic group G of an order q by means of a generator P, wherein the cyclic group G is an elliptic or hyper-elliptic curve Jacobian; (a2) producing a multiplicative cyclic group V of the order q by using a bilinear pairing e expressed as the following Equation: e: G*G->V (a3) determining cryptographic hash functions H: [0,1]*->Zq* and H1: {0,1}*->G; wherein Zq* is a multiplicative cyclic group corresponding to V; and (a4) selecting a master key s of the trusted authority and preparing a public key Ppub of the trusted authority by using the master key s and the generator P by using the following Equation Ppub=s.P (Figures 3-4 and 7, col. 5, line 60 through col. 6, line 56).

Regarding Claim 3, Boneh and Rivest disclose the limitations of Claim 2 above. Boneh further discloses wherein the set of system parameters has G, q, Ppub, P, H and H1 (col. 3, lines 30-45).

Regarding Claim 4, Boneh and Rivest A disclose the limitations of Claim 3 above. Boneh further discloses wherein the public key QIDi and the private key SIDi of the user are stored in a memory of the user, which are defined by using the following Equations: QIDi=H1(IDi) and SIDi=s.QIDi where IDi is the user's identity, i being a user index which is an integer ranging from 1 to n (col. 6, lines 25-45).

Regarding Claim 5, Boneh and Rivest disclose the limitations of Claim 4 above. Rivest further discloses wherein the step (d) includes the steps of: (d1) selecting an ID list L, wherein L is a set of identities of users; (d2) extracting a random element A of the cyclic group G, thereby computing an initial signature value by using the ID list L; (d3) choosing a random value of the cyclic group, thereby computing additional signature values by using the ID list L; (d4) generating a ring signature value by using the private key of the signer; (d5) forming a ring of ring signature values by selecting zero as a glue value of the additional signature values; and (d6) storing in a memory of the user the ID-based ring signature of n+1 ring signature values (pages 552-565).

Regarding Claim 6, Boneh and Rivest disclose the limitations of Claim 5 above. Boneh further discloses wherein, at the signer, the initial signature value, ck+1, is computed by using the following Equation: ck+1=H (L|| m || e(A, P)), wherein k is a signer index and m is the content-concealed message (Abstract, col. 4, lines 15-30).

Regarding Claim 7, Boneh and Rivest disclose the limitations of Claim 6 above. Boneh further discloses wherein an additional signature value is computed by using the following Equation: ci+1=H(L|| m || e(Ti, P)e(ciH1(IDi), Ppub)) for "i" corresponding to one of values of all modulo n (k+1, . . . , n-1, 0, 1 and k-1), and then stored in a memory of the signer wherein Ti is the random value of the cyclic group G (col. 29, lines 1-10).

Regarding Claim 8, Boneh and Rivest disclose the limitations of Claim 7 above. Boneh further discloses wherein the ring signature value, Tk, is calculated by using the following Equation: Tk=A-ckSIDk; and stored in a memory of the signer (Figures 10-12, elements 1106, 1107, col. 30, line 1 through col. 33, line 4).

Regarding Claim 9, Boneh and Rivest disclose the limitations of Claim 8 above. Boneh further discloses wherein the ID-based ring signature is a sequence (c0, T0, T1, . . . , Tn-1), which is stored in a memory of the user (Figures 10-12, elements 1106, 1107).

Regarding Claim 10, Boneh and Rivest disclose the limitations of Claim 9 above. Rivest further discloses wherein the validity of the ID-based ring signature is determined by using the following Equations:

$$c_{k+1} = H(L \| m \| e(A, P))$$

$$c_{k+2} = H(L \| m \| e(T_{k+1}, P)\, e(c_{k+1} H_1(ID_{k+1}), P_{pub}))$$

$$c_n = H(L \| m \| e(T_{n-1}, P)\, e(c_{n-1} H_1(ID_{n-1}), P_{pub}))$$

$$c_1 = H(L \| m \| e(T_0, P)\, e(c_0 H_1(ID_0), P_{pub}))$$

$$c_2 = H(L \| m \| e(T_1, P)\, e(c_1 H_1(ID_1), P_{pub}))$$

$$c_k = H(L \| m \| e(T_{k-1}, P)\, e(c_{k-1} H_1(ID_{k-1}), P_{pub}))$$

wherein if i=0, 1, . . . , n-1 and cn=cO, then the ID-based ring signature is determined to be valid; and if otherwise, the ID-based ring signature is rejected (pages 552-565).

Regarding Claim 12, Boneh and Rivest disclose the limitations of Claim 11 above. Boneh and Rivest further disclose the system parameters includes:a cyclic group G; G's order q; G's generator P; the trusted authority's public key Ppub described by Ppub=s.P, where s is the master key (Figures 3-4 and 7, col. 5, line 60 through col. 6, line 56 of Boneh); and

hash functions H and H1 described by H: {0,1}->Zq* and H1: {0,1}->G, where Zq* is a cyclic multiplicative group, wherein the bilinear pairings e are defined by e: G*G->V, where V is a cyclic multiplicative group of the order q and uses cyclic multiplicative group Zq* (col. 3, lines 30-45 of Boneh),

the user's public key QIDi is described by QIDi=H1(IDi), where IDi is the user's identity, i being a user index which is an integer ranging from 1 to n, the user's private key SIDi is described by SIDi=s.QIDi (col. 6, lines 25-45 of Boneh),

the initial signature value is computed by ck+1=H(L ||m || e (A, P)), where k is a signer index, L is a set of identities of users, m is a content-concealed message to be ring-signed and A is a random element of the cyclic group G (Abstract, col. 4, lines 15-30 of Boneh),

the additional signature values are generated by ci+1=H(L ||m || e (Ti, P)e(ciH1(IDi), Ppub)), for "i" corresponding to one of values of all modulo n (k+1, . . . , n-1, 0, 1, k-1), where Ti is a random value of the cyclic group G (col. 29, lines 1-10 of Boneh),

the ID-based ring signature value, Tk, is calculated by Tk=A-ckSIDk (Figures 10-12, elements 1106, 1107, col. 30, line 1 through col. 33, line 4 of Boneh),

the ID-based ring signature is obtained in a form of a sequence (c0, T0, T1, . . . , Tn-1) (Figures 10-12, elements 1106, 1107 of Boneh), and

the validity of the ID-based ring signature is determined by means of the following Equations:

$$c_{k+1} = H(L \| m \| e(A, P))$$

$$c_{k+2} = H(L \| m \| e(T_{k+1}, P)\, e(c_{k+1} H_1(ID_{k+1}), P_{pub}))$$

$$c_n = H(L \| m \| e(T_{n-1}, P)\, e(c_{n-1} H_1(ID_{n-1}), P_{pub}))$$

$$c_1 = H(L \| m \| e(T_0, P)\, e(c_0 H_1(ID_0), P_{pub}))$$

$$c_2 = H(L \| m \| e(T_1, P)\, e(c_1 H_1(ID_1), P_{pub}))$$

$$c_k = H(L \| m \| e(T_{k-1}, P)\, e(c_{k-1} H_1(ID_{k-1}), P_{pub}))$$

wherein if i=0, 1, . . . , n-1 and cn=c0, then the ID-based ring signature is accepted to be valid; and if otherwise, the ID-based ring signature is rejected (pages 552-565 of Rivest).

Contact Information

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT
01/30/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100